CMMC Compliance Checklist

Tips and tools for completing your first assessment...and five common pitfalls to avoid.

EGNYTE

Introduction

As part of a wider effort to protect its supply chain and the Defense Industrial Base (DIB) against cybersecurity threats, the U.S. Department of Defense will incorporate Cybersecurity Maturity Model Certification (CMMC) into RFIs starting in 2023.

That means that, if your company does work for the U.S. Department of Defense, or one of its agencies, in any way, you need to be planning for CMMC now.

Timeline as of October 2022:

CURRENT	Voluntary Self Assessments with CMMC Third Party Assessment Organizations (C3PAO's).
MAR 2023	Anticipated date for CMMC 2.0 Interim Rule public comment period to begin. Interim Rule will define the date at which DoD can begin requiring CMMC compliance in its solicitations.
MAY 2023	Anticipated date for CMMC to go into effect.
JULY 2023	Anticipated date that CMMC requirements will be included in DoD contracts.

Thankfully, the DoD's benchmarks are all achievable with proper planning and execution. In this ebook, you'll find a checklist and list of resources to support your implementation, and learn some of the common pitfalls to avoid.

What is CMMC?

The CMMC framework is based on assessments scored against the NIST SP 800-171 requirements.

There are three levels of compliance, each with its own set of practices companies must adhere to.

LEVEL 1	is foundational and has 17 practices to follow. It requires self-assessment and is intended for companies that handle Federal Contract Information (FCI) only.
LEVEL 2	is more advanced and is intended for companies that also handle Controlled Unclassified Information (CUI). It consists of 110 practices and requires triennial third-party assessments.
LEVEL 3	is expert and uses 110+ practices. It is more rigorous and requires formal government assessments.

At a high level, each of the practices outlined in CMMC falls under one of six core areas:

- Roles and responsibilities for IT security personnel, senior management, risk management
- Access control for CUI across your organization and measures to prevent unauthorized access to that data
- Partner relationships, including vendor onboarding and offboarding and any evaluation of those partners' cybersecurity postures
- Incident response, including how incidents are reported, tracked and reviewed
- Business continuity plans for how you expect to recover from a security incident or natural disaster
- Training and education of staff on the security measures and policies implemented

Download a spreadsheet containing the full requirements here, or visit the DoD's web site for more information at https://www.acq.osd.mil/cmmc/.

What is CUI and FCI?

Most organizations have more CUI and FCI than they realize. As a result, properly identifying sensitive information is typically the first challenge with CMMC.

CUI, which is government created or owned information, is supposed to be identified and labeled, but it frequently slips through without being categorized appropriately. Further, it can be created in your own company—not just by the DoD. Most examples are predictable, but some may surprise you.

These include:

- Building drawings on military bases including floor plans, electrical, plumbing, HVAC, etc.
- Personal information on DoD employees including contact, financial, health, and location
- IT security information itself, including configurations and architecture
- Product or service specifications and delivery schedules
- Time-based information for products and services including ordering patterns and trends
- Meeting schedules with DoD personnel and contractors
- Delivery locations

Federal Contract Information (FCI) is typically easier to identify. It includes:

- Contract terms and conditions
- Contract payment and delivery schedules
- Previous versions of contracts and markups

Your Compliance Checklist

- [ ] Verify that CMMC Applies to Your Organization
- [ ] Decide on Maturity Level
- [ ] Select a Project Lead
- [ ] Define Scope of CMMC Environment
- [ ] Engage Your Executive Team and Confirm Budget for CMMC
- [ ] Document Your Environment and Controls (System Security Plan: SSP)
- [ ] Assess Your Supply Chain and Partners
- [ ] Determine Who Handles CUI in Your Organization
- [ ] Deploy A Secure Enclave for Handling CUI
- [ ] Identify and Move CUI into the Enclave
- [ ] Develop Policies and Train Employees
- [ ] Define Compliance Review-and-Approval Workflows
- [ ] Conduct Your Self-Assessment
- [ ] Create and Submit Plan of Action and Milestones (POAM)

VERIFY THAT CMMC APPLIES TO YOUR ORGANIZATION

The first step is to determine whether you are required to comply with CMMC at all. In general, if your organization does any business with the U.S. Department of Defense, then you are part of the Defense Industrial Base (DIB) and may be subject to CMMC requirements as part of your contract if you handle CUI/FCI. How will you know for sure? Compliance requirements, including level, will appear as language in your contract. (See the official DoD FAQ for more information.)

Even if the DoD does not represent a majority of your business, you may still handle FCI in flow-down contracts, and CUI such as specifications and delivery schedules for products and services supplied to the DoD.

DECIDE ON MATURITY LEVEL

The CMMC levels represent an escalating set of commitments for certification, so you'll want to determine which one is appropriate for your business needs. If you only handle FCI, you'll need to comply with Level 1. If you handle both FCI and CUI information, you may need to comply with Level 2. Finally, if you are participating in larger contracts with more sensitive products and services, you may need to comply with Level 3.

Typically, your responsibility for compliance and the appropriate level will be explicitly spelled out in contracts and purchase agreements, either directly from the DoD, or via a flow-down contract if you are a subcontractor. You'll want to confirm with the contracting authority if it's not clear.

SELECT A PROJECT LEAD

Once you determine the level you will need to comply with, you'll need to identify or appoint a CMMC Lead within your organization, and provide the lead with significant executive support. They will be the champion for the project and work with outside consultants as necessary. The person in that role will need to develop a high-level of understanding of the CMMC requirements.

Larger organizations may want to dedicate a small team to CMMC compliance. As you assign members to the team, a best practice is to do it along the lines of the NIST SP 800-171 categories.

DEFINE SCOPE OF CMMC ENVIRONMENT

Defining the scope of the infrastructure included for CMMC compliance is critical. If defined too broadly, you'll incur additional costs and complexity, but if defined too narrowly, your users will be unable to work effectively. The scope includes not only the repository actually holding the CUI/FCI, but also associated services such as Identity and Access Management. Your System Security Plan (SSP) will then need to document the scope precisely so that auditors can determine which systems are in or out of scope. The DoD has provided guidance for scoping Level 1 Compliance here, and for scoping for Level 2 Compliance here.

ENGAGE YOUR EXECUTIVE TEAM AND CONFIRM BUDGET FOR CMMC

CMMC certification can be complex and expensive, so you'll want to begin the process with your executive team at this point to establish a budget for CMMC compliance.

This will likely depend on the value of current and future DoD contracts to your organization. However, because CMMC compliance consists of best practice cybersecurity processes, there will be intangible benefits as well. As your team learns and implements CMMC best practices, you'll reduce cybersecurity risk to your organization, at large.

DOCUMENT YOUR ENVIRONMENT AND CONTROLS (THE SSP)

According to NIST, the System Security Plan (SSP) "..describes: the system boundary; operational environment; how security requirements are implemented; and the relationships with or connections to other systems." In other words, it is a formal, written plan that documents the infrastructure (within scope), associated risks, and security controls in place (or planned) to mitigate those risks.

When it comes time for your assessment, you will need to produce complete documentation on the system under control. This calls for clearly defined and documented boundary diagrams, network architectures, services, and data flows for CUI, as well as documented processes and procedures for dealing with it. Getting started with the security control review early provides a baseline for the project and an early indication of your largest gaps.

Virtually no small- or mid-sized company has existing documentation to the depth and complexity required. Most often major components of the architecture are outsourced, and no documentation exists. Larger companies may have the people and documentation in-house, but the information can be spread across multiple IT teams rather than consolidated into one document. Whether big or small, the key point here is that you need a comprehensive inventory of exactly what falls into scope, who is responsible for each control, and how it's managed.

ASSESS YOUR SUPPLY CHAIN AND PARTNERS

As part of this step, you must reach out to external partners and notify them of your intent to become CMMC compliant. And importantly, determine if they are compliant.

Your subcontractors may not be required to be compliant initially, but over time, DoD and other government contracts will begin reaching further back into the supply chain. It's good for your subcontractors and partners to be aware of the trend, and to acknowledge that CMMC requirements are good cybersecurity practices to follow even before compliance is required.

DETERMINE WHO HANDLES CUI IN YOUR ORGANIZATION

Make a list of who needs access to CUI data to do their jobs in your organization. This may include individuals in legal, finance, sales, and technical areas, but depending on your situation, may not include everyone in those departments. CUI data should be assumed to be handled on a "need to know" basis.

This list will continue to change as people change roles, but it will be the starting point to set up permissions in a secure enclave for CUI data.

DEPLOY A SECURE ENCLAVE FOR HANDING CUI

Because the scope of the infrastructure is so critical to successful CMMC compliance, most organizations deploy a separate, highly secure system referred to as a "Secure Enclave" within their larger environment to store CUI/FCI information. This allows more careful control and monitoring of the way the information is accessed and used by limiting the "surface area". Most importantly, this greatly simplifies the burden of demonstrating compliance.

IDENTIFY AND MOVE CUI INTO THE ENCLAVE

Based on the contract and standard definitions, you'll need to identify what CUI data is (likely) in your organization. At this stage, make sure the obvious CUI is marked appropriately. You'll know which contracts and projects generate CUI data so that will be your starting point.

However, it's quite likely that CUI data has "leaked" into other parts of your organization, so you will need to perform a mapping exercise to find that data, and then move it into the enclave. A data classification solution may be required to help locate CUI in repositories such as Microsoft SharePoint sites, file servers and email system (Egnyte provides such a solution as a complement to its secure enclave product).

DEVELOP POLICIES AND TRAIN EMPLOYEES

CMMC is not just about protecting data, it's also about how to use that data safely. You'll need to develop internal policies that cover who/how/when CUI data can be accessed. You'll need to define how it is to be used and modified, and most importantly, what is not allowed. For example, some organizations find it necessary to limit printed copies. They also need to limit replication of the data on unsecured laptops. Once employees who deal with CUI data have been identified, you will need to train them on proper procedures for safe handling and management of CUI data. It's also helpful to train all employees to be aware of CUI even if they are not expected to handle it. This training should be done on a routine basis—not just for new employees, but to help reinforce best practices for existing employees, too.

DEFINE COMPLIANCE REVIEW-AND-APPROVAL WORKFLOWS

As you get closer to completing your assessment, you'll need to set up the workflow for reviews and approvals of the various components of the project. Identify who will be responsible for capturing the actual compliance artifacts, who will review them, and who will provide final approval. Note that there are at least 110 practices to comply with at Level 2 and 3, so compliance with the practices represents a significant resource commitment.

CONDUCT YOUR SELF-ASSESSMENT

Once the System Security Plan (SSP) has been outlined, it will be necessary to do a self-assessment. This is the point where you'll identify the gaps in your coverage of security controls, as you fill out the assessment document. Note that some items may not be applicable to your situation. For example, if you use a cloud-based solution and your employees are remote, you may not need to worry about physical access controls such as visitor escorts (PE.L1-3.10.3). However, you'll still need to explain why that is the case.

In the event your solution does have controls in place to meet a requirement, you'll need to demonstrate that with documentation including screenshots, written policies, or other information (admins of Egnyte's secure enclave solution can auto-generate this documentation from a dashboard within the product). This is true whether you assemble the control yourself, or whether it is inherited from a solution you purchased. Finally, almost all organizations discover gaps in coverage of security controls that will need to be addressed in the future. These need to be carefully documented with a plan to address them including a budget and schedule.

CREATE AND SUBMIT PLAN OF ACTION AND MILESTONES (POAM)

A Plan of Action and Milestones (POAM) will be your response to any gaps in control coverage discovered during the self assessment. It details resources (People, Process, Technology) required to address the missing control. In the case of a complex project, it should include intermediate milestones with scheduled completion dates for the milestones. Note that a POAM may be used to respond to minor control gaps for a formal audit, but may not be accepted if used for major control deficiencies. In any case, follow-through is important. Auditors may request confirmation when the project is complete.

Common Pitfalls to Avoid

When implementing your CMMC checklist, here are some of the most common pitfalls to avoid.

1. WAITING TOO LONG

Many organizations assume that CMMC compliance can be achieved in a short period, perhaps as little as a week or two, because they already have cybersecurity policies and practices in place.

However, experience has shown that even the most sophisticated organizations can take months to achieve and document compliance. This is because CMMC compliance is more than just an IT exercise and requires more than just a technology fix. First, detailed planning is required, often leading to additional technology. Additionally, remember that all employees will need to be trained, while new processes and procedures will need to replace old ones. This all requires executive level engagement, not just spending approvals.

2. SCOPING TOO BROADLY

Out of an abundance of caution, security engineers can sometimes be more inclusive than they need be in defining the scope of the infrastructure to fall under CMMC. In rare cases, they may mis-define CUI too broadly, so data is listed as CUI when it isn't. More often, they simply don't know where their CUI is, so they include more infrastructure than is necessary. This can lead to including multiple repositories in scope, and associated infrastructure and network capabilities like Identity and Access Management (IAM) services across many different systems. A broader scope results in a much more complex and expensive path to CMMC.

Likewise, engineers sometimes target a higher CMMC level than necessary, striving for Level 2 when Level 1 is sufficient for their FCI data. Like scoping the infrastructure too broadly, striving for unnecessary levels of CMMC compliance multiplies cost, complexity, and resources. Even if Level 2 compliance is necessary, it might be more practical and less disruptive to do Level 1 compliance first before attempting Level 2 compliance.

Another, even more subtle, scoping problem is a failure to include partners and supply chain participants in planning for CMMC compliance. For example, unique specifications sent to a supplier may contain CUI data. Therefore, that partner should be notified that they may need to comply with CMMC requirements as well. At the very least, the information needs to be passed in a secure way and employees trained on proper handling.

3. LACK OF DETAIL

When working through checklists, companies sometimes don't spend enough time documenting the details on key focus areas in the requirements. For example, logging should be documented to show not only that logs are collected, but also how often they are collected, how they are stored, and most importantly, how they are reviewed and analyzed. Likewise, access controls may be neglected in detailed documentation because they are complex and cross many different internal system boundaries. Documentation of access controls should include not only how they work, but the processes for how they are maintained and verified.

Finally, many security engineers often leave out detailed documentation on procedures, both for admins configuring and monitoring the system as well as users handling CUI data itself. It's important to document proper procedures so that deviations from normal processes can be detected quickly before data is put at risk.

4. LACK OF CONTINUOUS MONITORING

Many organizations struggle to "climb the CMMC mountain" only to relax and become complacent at the top. CMMC requires continuous review, monitoring and improvement. The best way to do this is to choose tools and architectures (like Egnyte) that allow you to automate as much of the ongoing monitoring and maintenance as possible.

5. VIEWING CMMC AS JUST A ONE-TIME EVENT

CMMC compliance is not a one-time event or checklist exercise. In reality, it affects people, processes, and technology, often profoundly. Your people may need significant training, cultures need to be modified, new processes and procedures and even business workflows may need to change.

Technology needs to support the new requirements, but these deployments should never be regarded as a static state. Over time, your business will change, which changes your risk profile and attack surface. Meanwhile, new security risks will continue to emerge, and cybersecurity solutions will evolve with them. Therefore, your SSP will need frequent review and updating to meet those risks.

This is why the DoD plans for CMMC audits to be performed on a regular basis rather than one time. CMMC compliance truly is a journey, not a destination.

How Egnyte Helps Companies On Their CMMC Journey

Egnyte provides a simple, secure data environment specifically designed to make compliance practical and affordable for small- and mid-sized businesses.

The Egnyte for CMMC solution will save your IT and compliance teams weeks, if not months, of time each year. Meanwhile, business stakeholders will appreciate that it's easy to use and enables them to win/maintain DoD contracts while minimizing the amount of overhead (including third-party consulting hours) required to do so.

Egnyte's secure enclave satisfies many CMMC requirements by default. The solution also includes advanced governance capabilities to help you discover CUI/FCI in third-party repositories (such as Microsoft SharePoint, Microsoft Exchange, and on-prem file servers) allowing you to limit the scope of the auditable environment. When it comes time to prepare your next assessment, you simply click a few buttons in Egnyte's reporting interface to auto-generate much of the documentation that will be needed.

1	Secure Enclave With Inherited CMMC Controls (see Shared Responsibility Matrix on the following page)
2	Detailed Technical Integration and Configuration Guide
3	Tools to Locate and Label Data In 3rd Party Repositories
4	Auto-Generated Artifacts and Responses
5	Access to Practitioner Community
6	Access to Egnyte's CMMC Experts
7	Unbiased Partner Recommendations (C3PAOs, consultants, etc.)

Egnyte for CMMC Shared Responsibility Matrix

CMMC 2.0 Practice / NIST SP 800-171 Security Requirement	Controls Inherited from Egnyte for CMMC's IaaS Provider	Egnyte for CMMC Platform Settings	Egnyte for CMMC SaaS Supporting Control	Total Number of Controls Required by NIST SP 800-171
CMMC 2.0 Access Control (AC) Practices	0	12	3	22
CMMC 2.0 Awareness and Training (AT) Practices	0	0	0	3
CMMC 2.0 Audit and Accountability (AU) Practices	1	3	3	9
CMMC 2.0 Configuration Management (CM) Practices	4	0	8	9
CMMC 2.0 Identification and Authentication (IA) Practices	2	9	6	11
CMMC 2.0 Incident Response (IR) Practices	0	0	3	3
CMMC 2.0 Maintenance (MA) Practices	6	0	3	6
CMMC 2.0 Media Protection (MP) Practices	0	0	1	9
CMMC 2.0 Personnel Security (PS) Practices	0	0	0	2
CMMC 2.0 Physical Protection (PE) Practices	6	0	0	6
CMMC 2.0 Risk Assessment (RA) Practices	0	0	3	3
CMMC 2.0 Security Assessment (CA) Practices	0	0	3	4
CMMC 2.0 System and Communications Protection (SC) Practices	3	4	8	16
CMMC 2.0 System and Information Integrity (SI) Practices	0	1	5	7
TOTALS	**22**	**29**	**46**	**110**

To learn more, visit: https://www.egnyte.com/solutions/cmmc-compliance

Appendix: Additional Links and Resources

Authoritative guidance for CMMC comes from the Department of Defense itself at: https://www.acq.osd.mil/cmmc/

There, you'll find useful information on the CMMC Model itself including:

- Model Overview
- CMMC 2.0 Spreadsheet and Mapping
- A CMMC Glossary

As you begin your CMMC journey, you'll need to understand how to properly scope the infrastructure that requires compliance. The DoD has assembled these resources for that:

- CMMC Level 1 Scoping Guidance
- CMMC Level 2 Scoping Guidance

Then you'll use assessment guides for your self-assessment. These are located here:

- CMMC Level 1 Self-Assessment Guide
- CMMC Level 2 Assessment Guide

(Note that CMMC Level 3 assessment is still under development as of this writing.)

The NIST document that the DoD uses as the basis for CMMC is NIST SP 800-171 (Rev 2) can be accessed here: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Schedule a CMMC Workshop

If you have additional questions about CMMC compliance, Egnyte is here to help. Reach out to your Egnyte representative to schedule a CMMC Workshop, where we can discuss your company's CMMC journey in further detail, or click here.

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com